MATHEMATICAL COMMUNICATIONS
Math. Commun. **17**(2012), 639–654

Constructions for uniform $(m, 3)$-splitting systems

Dongyoung Roh[1,*] and Sang Geun Hahn[2]

[1] *Attached Institute of Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea*
[2] *Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea*

Received October 7, 2011; accepted June 2, 2012

Abstract. Suppose m and t are integers such that $0 < t \leq m$. An (m, t)-splitting system is a pair $(X, \mathbb{B})$, where $|X| = m$ and $\mathbb{B}$ is a set of subsets of X, called blocks, such that for every $Y \subseteq X$ and $|Y| = t$, there exists a block $B \in \mathbb{B}$ such that $|B \cap Y| = \lfloor t/2 \rfloor$. An (m, t)-splitting system is uniform if every block has size $\lfloor m/2 \rfloor$. We present new construction methods of uniform splitting systems for $t = 3$ that have a smaller number of blocks as compared to previous results.
AMS subject classifications: 05B20, 94A60
Key words: splitting systems, baby-step giant-step algorithms, low Hamming weight discrete logarithm problem

1. Introduction

Splitting systems were used by Stinson [3] in baby-step giant-step algorithms for the low hamming weight discrete logarithm problem. It is known that the smaller the splitting systems are, the better the algorithms are.

In 2004, Ling, Li and van Rees presented results on uniform splitting systems for $t = 2$ and 4 using their newly obtained results for separating systems [2]. Later, Deng, Stinson, Li, van Rees, and Wei gave several constructions and bounds for splitting systems for $t = 3$ [1]. In this paper, we present some new results on uniform splitting systems for $t = 3$ that improve upon the previous results in [1].

We begin with the definitions of a splitting system and a uniform splitting system.

Definition 1. *Let m and t be integers greater than* 1. *An* (m, t)-splitting system *is a set system $(X, \mathbb{B})$ that satisfies the following properties:*

1. *X is a finite set of* m points *(i.e., $|X| = m$).*
2. *$\mathbb{B}$ is a collection of subsets of X, called* blocks.
3. *For every $Y \subseteq X$ with $|Y| = t$, there exists a block $B \in \mathbb{B}$ such that $|B \cap Y| = \lfloor \frac{t}{2} \rfloor$.*

We will use the notation $(N; m, t)$-SS to denote an (m, t)-splitting system having N blocks.

*Corresponding author. *Email addresses:* dyrohnsri@ensec.re.kr (D. Roh), sghahn@kaist.ac.kr (S. G. Hahn)

Definition 2. *Let m and t be integers greater than* 1. *A* uniform (m,t)-splitting system *is an (m,t)-splitting system in which every block has cardinality $\lfloor \frac{m}{2} \rfloor$. We will use the notation $(N;m,t)$-uniform SS to denote a uniform (m,t)-splitting system having N blocks.*

For convenience in constructing the splitting systems, we define the incidence matrix of a splitting system as follows.

Definition 3. *Let $(X,\mathbb{B})$ be an $(N;m,t)$-SS, where $X = \{x_j : 1 \le j \le m\}$ and $\mathbb{B} = \{B_i : 1 \le i \le N\}$. The* incidence matrix *of $(X,\mathbb{B})$ is an $N \times m$ matrix $A = (a_{i,j})$ where*

$$a_{i,j} = \begin{cases} 1, \text{ if } x_j \in B_i; \\ 0, \text{ otherwise.} \end{cases}$$

We present an example of a uniform splitting system.

Example 1.

$$\begin{pmatrix} 1&1&1&1&1&0&0&0&0&0 \\ 0&1&1&1&0&1&1&0&0&0 \\ 1&1&0&0&0&1&1&1&0&0 \\ 0&0&0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&0&0&1&1&1 \end{pmatrix}$$

is the incidence matrix of a $(5;10,3)$-uniform SS.

The following is a very useful lemma to determine whether the given set system is a splitting system with $t = 3$ using the incidence matrix of the system. It is due to Deng, Stinson, Li, van Rees, and Wei [1].

Lemma 1. *Suppose that $A = (a_{i,j})$ is an $N \times m$ matrix having entries in the set $\{0,1\}$. Then, A is the incidence matrix of an $(N;m,3)$-SS if and only if, for all choices of three columns c_1, c_2, c_3 of A, the following property is satisfied:*

$$\text{There is a row } r \text{ such that } (a_{r,c_1}, a_{r,c_2}, a_{r,c_3}) \in \{(0,0,1),(0,1,0),(1,0,0)\} \qquad (1)$$

The remainder of this paper is organized as follows. In Section 2, we present the preliminary results on uniform splitting systems. In Section 3, we describe a new construction method for uniform $(m,3)$-splitting systems when m is odd. In section 4, we provide another construction method for uniform $(m,3)$-splitting systems different from that of Section 3. Finally, we conclude in Section 5.

2. Preliminary results

In this section, we review some preliminary results on the number of blocks of uniform $(m,3)$-splitting systems. First, we give a general lower bound for a (m,t)-splitting system. It is due to Deng, Stinson, Li, van Rees and Wei [1].

Theorem 1. *For all $m \ge t+1$, an (m,t)-splitting system has at least $\lfloor \log_2(m - t + 1) \rfloor + 1$ blocks.*

The following two theorems pertain to the upper bounds for the number of blocks of uniform $(m,3)$-splitting systems [1]. We only give the constructions methods.

Theorem 2. *Let $m \geq 4$ be even. Then there exists an $(N;m,3)$-uniform SS, with $N = 2\lceil \log_2 m \rceil - 2$.*

Proof. Denote $l = \lceil \log_2 m \rceil - 2$. Construct an $l \times m/2$ binary matrix, named T_m, as follows. The columns of T_m are (in order) $c_0, \ldots, c_{m/2-1}$, where

$$c_i = \begin{cases} \text{the binary representation of } i, & \text{if } i \leq 2^l - 1; \\ \text{the binary representation of } i - 2^l, & \text{if } 2^l \leq i \leq m/2 - 1. \end{cases}$$

Each c_i is a column vector of length l.

Now construct a $(2l+2) \times m$ matrix A as follows:

$$A = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \\ \hline T_m & T_m^c \\ \hline T_m^c & T_m \end{array}\right),$$

where T_m^c is the complement of T_m (i.e., every entry "0" is replaced by "1" and vice versa). Here and elsewhere, **1** and **0** denote row or column vectors of "1"s and "0"s, respectively. □

Theorem 3. *For any odd integer $m \geq 7$, there exists an $(N;m,3)$-uniform SS where $N \leq 2\lceil \log_2(m-3) \rceil + 2$.*

Proof. Denote $m' = m - 3$. Construct the $(\lceil \log_2 m' \rceil - 2) \times m'/2$ matrix $T_{m'}$ as in Theorem 2. Then construct the following incidence matrix A:

$$A = \left(\begin{array}{c|c|c} \mathbf{1} & \mathbf{0} & 1\ 0\ 0 \\ \mathbf{0} & \mathbf{1} & 1\ 0\ 0 \\ \mathbf{1} & \mathbf{0} & 0\ 1\ 0 \\ \mathbf{0} & \mathbf{1} & 0\ 1\ 0 \\ \mathbf{1} & \mathbf{0} & 0\ 0\ 1 \\ \mathbf{0} & \mathbf{1} & 0\ 0\ 1 \\ \hline T_{m'} & T_{m'}^c & 0\ 0\ 1 \\ \hline T_{m'}^c & T_{m'} & 0\ 0\ 1 \end{array}\right)$$

□

Next, we observe that we can construct a uniform $(2m,3)$-splitting system from a uniform $(m,3)$-splitting system for even m as follows [1].

Theorem 4. *Suppose that m is even. If there exists an $(N;m,3)$-uniform SS, then there exists an $(N+2;2m,3)$-uniform SS.*

Proof. Let A be the $N \times m$ incidence matrix of the $(N;m,3)$-uniform SS. We construct the incidence matrix of the uniform $(2m,3)$-splitting system on $(N+2)$ blocks as follows:

$$A' = \left(\begin{array}{c|c} A & A \\ \hline \mathbf{1} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{1} \end{array}\right)$$

□

3. Constructions for uniform $(m, 3)$-SS when m is odd

In this section we present a new construction method for $(m, 3)$-uniform splitting systems when m is odd. This method improves upon the result of Theorem 3.

First, we give two examples of uniform $(m, 3)$-splitting systems. They will be used in the proof of the following theorems.

Example 2.

$$\begin{pmatrix} 1&1&1&0&0&0&0\\ 1&0&0&1&1&0&0\\ 1&0&0&0&0&1&1 \end{pmatrix}$$

is the incidence matrix of a $(3; 7, 3)$*-uniform SS.*

Example 3.

$$\begin{pmatrix} 1&1&1&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&1&1&1&1&0&1\\ 1&1&0&0&0&1&1&0&0&1&0\\ 0&1&1&0&0&0&0&1&1&0&1\\ 0&1&0&1&1&0&1&0&1&0&0 \end{pmatrix}$$

is the incidence matrix of a $(5; 11, 3)$*-uniform SS.*

We now give an upper bound for a uniform $(m, 3)$-splitting system when m is odd. This upper bound is lower than that of Theorem 3. We prove this by dividing it into three cases. In the first case, $(m - 3)$ is a power of 2.

Theorem 5. *For any integer* $n \geq 2$*, there exists a* $(2n - 1; 2^n + 3, 3)$*-uniform SS.*

Proof. By Examples 2 and 3, the theorem is true for $n = 2, 3$. We prove the theorem by using mathematical induction. Let's assume that there exists a $\left(2k - 1; 2^k + 3, 3\right)$-uniform SS for $k \geq 3$. Let A_{2^k+3} denote its incidence matrix. Also, there exists a $\left(2k - 2; 2^k, 3\right)$-uniform SS by Theorem 2. Let A_{2^k} denote its incidence matrix.

By changing positions of rows and columns in A_{2^k+3}, we obtain the following matrix A'_{2^k+3} that is also an incidence matrix of a $(2k - 1; 2^k + 3, 3)$-uniform SS (later in this proof, we will show that A_{2^k+3} contains the last two columns of A'_{2^k+3}):

$$A'_{2^k+3} = \left(\begin{array}{c|cc} B_1 & \mathbf{0} & \mathbf{0}\\ B_2 & \mathbf{0} & \mathbf{1}\\ B_3 & 1 & 0\\ B_4 & 0 & 1\\ B_5 & 0 & 0 \end{array}\right)$$

where B_1 and B_2 denote $(k - 2)$ by $\left(2^k + 1\right)$ submatrices of A'_{2^k+3} and B_3, B_4, and B_5 denote 1 by $\left(2^k + 1\right)$ submatrices of A'_{2^k+3}.

Now construct a $(2k + 1) \times \left(2^{k+1} + 3\right)$ matrix A as follows:

$$A = \left(\begin{array}{c|c|c||c|c} B_1 & \mathbf{0} & \mathbf{0} & T_{2^k} & T^c_{2^k} \\ B_2 & \mathbf{0} & \mathbf{1} & T^c_{2^k} & T_{2^k} \\ B_3 & 1 & 0 & \mathbf{0} & \mathbf{1} \\ B_4 & 0 & 1 & \mathbf{1} & \mathbf{0} \\ \hline B_5 & 0 & 0 & \mathbf{1\ 0} & \mathbf{0\ 1} \\ \hline \mathbf{1} & 0 & 0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 1 & \mathbf{1} & \mathbf{1} \end{array}\right),$$

where the matrix obtained by taking the first $(2k-1)$ rows and the first $\left(2^k+3\right)$ columns is A'_{2^k+3}, and T_{2^k} is the $(2k-2) \times \left(2^k\right)$ matrix we used in the proof of Theorem 2. Also, $\mathbf{1}$ and $\mathbf{0}$ in the $(2k-1)$-th row denote the row vectors of length 2^{k-2}. Let L_1 denote the first $\left(2^k+1\right)$ columns of A, let L_2 denote the next column of A, let L_3 denote the next column of A, let R_1 denote the next 2^{k-1} columns of A, and let R_2 denote the last 2^{k-1} columns of A. Note that the first $(2k-1)$ rows of L_2 and L_3 are parts of A'_{2^k+3} and the first $(2k-2)$ rows of R_1 and R_2 form a $\left(2k-2; 2^k, 3\right)$-uniform SS, as in the proof of Theorem 2.

First, we claim that we can construct the above matrix inductively. To construct the above matrix inductively, A_{2^k+3} should contain two kinds of columns. The first must have only one "1", and "0" elsewhere. There exists such column in the $(5; 11, 3)$-uniform SS of Example 3. The second must have $(k-1)$ "1"s and k "0"s, and the element of the row where the first kind of column that has "1" must be "0". There exist such column in the $(5; 11, 3)$-uniform SS of Example 3. In addition, the constructed matrix A above also has these two kinds of columns. Therefore, we can construct the above matrix inductively.

Now we prove that A is the incidence matrix of a $\left(2k+1; 2^{k+1}+3, 3\right)$-splitting system.

1. Three columns from $\{L_1, L_2, L_3\}$: If we delete the last two rows and the last 2^k columns of A, then we obtain the incidence matrix, A'_{2^k+3}, of a $\left(2k-1; 2^k+3, 3\right)$-uniform SS. Therefore, (1) is satisfied.

2. Three columns from $\{R_1, R_2\}$: If we delete the last three rows and the first $\left(2^k+3\right)$ columns of A, then we obtain the incidence matrix, A_{2^k}, of a $\left(2k-2; 2^k, 3\right)$-uniform SS. Therefore (1) is satisfied.

3. Two columns from L_1 and one column from $\{R_1, R_2\}$: Then (1) is satisfied by taking the last row of A.

4. One column from each L_1, $\{L_2, L_3\}$, and $\{R_1, R_2\}$: Then (1) is satisfied by taking the second last row of A.

5. The columns L_2, L_3, and one column from $\{R_1, R_2\}$: Then (1) is satisfied by taking one of the $(2k-2)$-th row and $(2k-3)$-th row of A.

6. One column from L_1 and two columns from $\{R_1, R_2\}$: Then (1) is satisfied by taking the second last row of A.

7. One column from each $\{L_2, L_3\}$, R_1, and R_2: Then (1) is satisfied by taking one of the $(2k-2)$-th row and $(2k-3)$-th row of A.

8. One column from $\{L_2, L_3\}$ and two columns from R_1: We call these three columns c_1, c_2, and c_3, respectively. If $|c_2 - c_3| \neq 2^{k-2}$, then there exists a row r in T_{2^k} such that $a_{r,c_2} \neq a_{r,c_3}$. Then (1) is satisfied, since $a_{r,c_1} = 0$. On the other hand, if $|c_2 - c_3| = 2^{k-2}$, then (1) is satisfied by taking the third last row of A.

9. One column from $\{L_2, L_3\}$ and two columns from R_2: The proof of this case is similar to the previous proof.

Finally, it is straightforward that each row of A has exactly $\left(2^k + 1\right)$ "1"s. Therefore, the splitting system is uniform. □

By using Theorem 5, we construct the incidence matrix of a $(7; 19, 3)$-uniform SS from the incidence matrix of a $(5; 11, 3)$-uniform SS in Example 3.

Example 4.

$$\left(\begin{array}{cccccccccc|c|c||cccc|cccc}
1&1&1&1&1&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0\\
0&0&0&0&0&1&1&1&1&1&0&1&1&0&1&0&0&1&0&1\\
1&1&0&0&0&1&1&0&0&1&1&0&0&0&0&0&1&1&1&1\\
0&1&1&0&0&0&0&1&1&0&1&1&1&1&1&1&0&0&0&0\\
\hline
0&1&0&1&1&0&1&0&1&0&0&1&1&0&0&0&0&0&1&1\\
\hline
1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1
\end{array}\right)$$

In the second case, $(m-1)$ is a power of 2. To prove the second case we give the following lemma that can be obtained from the splitting systems constructed by Theorem 5.

Lemma 2. *For any integer $n \geq 3$, there exists a $(2n-1; 2^n+3, 3)$-uniform SS whose incidence matrix has two columns such that one is the complement of the other.*

Proof. The lemma is true for $n = 3$ by Example 3. We show this by using the recursive construction method of Theorem 5 starting from Example 3. Actually, we show that the first column is the complement of the first column of R_1 in the matrix A (in terms of Theorem 5). For $n = 4$, we know that the first column is the complement of R_1 by Example 4.

Suppose that the first column is the complement of the first column of R_1 in A_{2^k+3}. Extract the last two rows of A_{2^k+3} and put these two rows between the $(k-3)$-th row and $(k-2)$-th row. Next, extract the $\left(2^{k-1}+2\right)$-th column and $\left(2^{k-1}+3\right)$ column and put these two columns after the last column. We can then construct $A_{2^{k+1}+3}$ using Theorem 5 without exchanging any rows or columns. It is easy to see that the first column of $A_{2^{k+1}+3}$ is the complement of the first column of R_1 of $A_{2^{k+1}+3}$. □

Now we can prove the second case using the above lemma.

Theorem 6. *For any integer $n \geq 3$, there exists a $(2n-1; 2^n+1, 3)$-uniform SS.*

Proof. By Lemma 2, we know that there exists a $(2n-1; 2^n+3, 3)$-uniform SS that has two columns such that one is the complement of the other. If we delete these two columns from its incidence matrix, we obtain the incidence matrix of a $(2n-1; 2^n+1, 3)$-uniform SS. □

Lastly, we prove the case where neither $\log_2(m-3)$ nor $\log_2(m-1)$ is an integer.

Theorem 7. *For any odd integer $m \geq 9$, there exists an $(N; m, 3)$-uniform SS where $N = 2\lceil \log_2(m-3) \rceil - 1$, if neither $\log_2(m-3)$ nor $\log_2(m-1)$ is an integer (i.e., there does not exist an integer n such that $m = 2^n + 3$ or $m = 2^n + 1$).*

Proof. Denote $m' = m - 3$ and $l = \lceil \log_2 m' \rceil - 2$. Construct an $l \times m'/2$ binary matrix, named $U_{m'}$, as follows. The columns of $U_{m'}$ are (in order) $c_0, \ldots, c_{m'/2-1}$, where

$$c_i = \begin{cases} \text{the binary representation of } (i+1), \text{ if } i \leq 2^l - 3 \\ \text{the binary representation of } \left(i + 3 - 2^l\right), \text{ if } 2^l - 2 \leq i \leq m'/2 - 1. \end{cases}$$

Each c_i is a column vector of length l.

Now construct a $(2l+3) \times m$ matrix A as follows:

$$A = \left(\begin{array}{c|c||ccc} \mathbf{0} & \mathbf{1} & 1 & 0 & 0 \\ \mathbf{1} & \mathbf{0} & 0 & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 & 0 \\ \hline U_{m'} & U^c_{m'} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \hline U^c_{m'} & U_{m'} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{array}\right).$$

Let L_1 denote the first $m'/2$ columns of A, let L_2 denote the next $m'/2$ columns of A, and let R_1, R_2, R_3 denote the last three columns of A, respectively.

Now we prove that A is the incidence matrix of a $(2\lceil \log_2(m-3) \rceil - 1; m, 3)$-splitting system.

1. Three columns from $\{L_1, L_2\}$: Note that if we delete the first row and the last three columns of A, then we obtain the incidence matrix of a $(2\lceil \log_2(m-3) \rceil - 2; m-3, 3)$-uniform SS. This can be proved by using the same argument as proved in Theorem 2. Therefore, (1) is satisfied.

2. Three columns R_1, R_2, and R_3: Then (1) is satisfied by taking the first row of A.

3. Two columns from L_1 and one column from $\{R_1, R_2\}$: Then (1) is satisfied by taking the first row or the third row of A.

4. Two columns from L_1 and the column R_3: We call these three columns c_1, c_2, and c_3, respectively. If $|c_1 - c_2| \neq 2^l - 2$, then there exists a row r in $U^c_{m'}$ such that $a_{r,c_1} \neq a_{r,c_2}$. Then (1) is satisfied, since $a_{r,c_3} = 0$. On the other hand, if $|c_1 - c_2| = 2^l - 2$, then there exists a row r in $U_{m'}$ such that $a_{r,c_1} = a_{r,c_2} = 0$. Then (1) is satisfied, since $a_{r,c_3} = 1$.

5. Two columns from L_2 and one column from $\{R_1, R_3\}$: Then the proof is similar to the previous case.

6. Two columns from L_2 and the column R_2: Then (1) is satisfied by taking the second row of A.

7. One column from each L_1, L_2, and $\{R_1, R_2, R_3\}$: Then (1) is satisfied by taking one of the first three rows of A.

8. One column from $\{L_1, L_2\}$ and two columns from $\{R_1, R_2, R_3\}$: Then (1) is satisfied by taking one of the first three rows of A.

To complete the proof, we observe that every row of A contains exactly $m'/2 + 1 = (m-1)/2$ "1"s. □

By combining the previous three theorems, we obtain the following result.

Theorem 8. *For any odd integer $m \geq 7$, there exists an $(N; m, 3)$-uniform SS where $N \leq 2\lceil \log_2(m-3) \rceil - 1$.*

4. Constructions for uniform $(m, 3)$-SS

In the previous section, we showed better construction methods than the previous results for uniform $(m, 3)$-splitting systems when m is odd . In this section, we present more construction methods for uniform $(m, 3)$-splitting systems for both odd and even m.

Suppose that there is an $(N; m, 3)$-nonuniform SS. Let A denote its incidence matrix. We can then obtain the incidence matrix of $(N; m-1, 3)$-nonuniform SS by deleting any column from A. However, it does not work when the splitting system is uniform. To perform a similar construction, we give the following definition.

Definition 4. *Suppose that there exists an $(N; m, 3)$-uniform SS and let A denote its incidence matrix. We say that the $(N; m, 3)$-uniform SS has k pairs of complementary columns if there exist x_i's and y_i's for $1 \leq i \leq k$ such that*

1. *$x_i, y_i \in \{1, 2, \ldots, m\}$,*

2. *x_i's and y_i's are all distinct, i.e., $|\{x_1, \ldots, x_k, y_1, \ldots, y_k\}| = 2k$,*

3. *for every $i \in \{1, \ldots, k\}$, $a_{j,x_i} \neq a_{j,y_i}$ for $1 \leq j \leq N$.*

Suppose that there exists an $(N; m, 3)$-uniform SS having k pairs of complementary columns. This means that we can obtain an $(N; m-2k, 3)$-uniform SS by deleting k pairs of complementary columns.

We prove our main theorem by dividing it into two cases, when m is odd and even. We first look at the case where m is even. To prove this case we need the following lemma which states the number of pairs of complementary columns of the splitting system constructed recursively when m is even.

Lemma 3. *For an even integer m, suppose that there exists an $(N; m, 3)$-uniform SS that has k pairs of complementary columns. Then there exists an $(N+2; 2m, 3)$-uniform SS that has $2k$ pairs of complementary columns.*

Proof. Let A denote the incidence matrix of an $(N;m,3)$-uniform SS that has k pairs of complementary columns. Then there exist x_i's and y_i's that satisfy the condition of Definition 4. We use the same construction method as in Theorem 4. Construct the incidence matrix of the $(N+2;2m,3)$-uniform SS as follows:

$$A' = \left(\begin{array}{c|c} A & A \\ \hline \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{array}\right).$$

We know that this is the incidence matrix of $(N+2;2m,3)$-uniform SS. Next, we show that this splitting system has $2k$ pairs of complementary columns. For every $1 \le i \le k$, $a'_{j,x_i} \ne a'_{j,y_i+m}$ and $a'_{j,x_i+m} \ne a'_{j,y_i}$ for $1 \le j \le N+2$. This means that each pair of complementary columns in the $(N;m,3)$-uniform SS gives two pairs of complementary columns in the $(N+2;2m,3)$-uniform SS. Hence, the third condition of Definition 4 is satisfied, and the other two conditions can be easily checked. Therefore, there exists an $(N+2;2m,3)$-uniform SS that has $2k$ pairs of complementary columns. □

We now show the even case of our main theorem.

Theorem 9. *For every integer $n \ge 3$, there exists a $(2n-1;2^n+2k,3)$-uniform SS where $0 \le k \le 2^{n-3}$.*

Proof. We know that there exists a $(5;10,3)$-uniform SS that has 3 pairs of complementary columns from Example 1. Therefore, by Lemma 3, there exists a $(2n-1;2^n+2^{n-2},3)$-uniform SS that has $3 \times 2^{n-3}$ pairs of complementary columns. If we delete $(2^{n-3}-k)$ pairs of complementary columns from the incidence matrix of a $(2n-1;2^n+2^{n-2},3)$-uniform SS, we obtain the incidence matrix of a $(2n-1;2^n+2k,3)$-uniform SS. □

Next, we prove the second case of our main theorem where m is odd. Before looking at the second case, we give an example that will be used in the following lemmas and theorem.

Example 5.

$$\left(\begin{array}{cccccccccc|c} 1&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&1&1&0&0&0&0 \\ 1&1&0&1&0&0&0&1&1&0&0 \\ 0&0&1&1&0&1&1&0&0&1&1 \\ 0&0&0&1&1&0&0&1&1&1&1 \end{array}\right)$$

is the incidence matrix of a $(5;11,3)$-SS. This is not a uniform SS. Note that the first 10 columns of this matrix form the incidence matrix of a $(5;10,3)$-uniform SS. This is an important property.

Before giving the second case of our main theorem, we give two lemmas that will be used in the proof of the theorem. The first lemma states that there exists a $(2n-1;2^n+2^{n-2}+1,3)$-SS containing a $(2n-1;2^n+2^{n-2},3)$-uniform SS for $n \ge 3$ as in the above example.

Lemma 4. *For any integer $n \geq 3$, there exists a $(2n-1; 2^n + 2^{n-2} + 1, 3)$-SS such that the first $\left(2^n + 2^{n-2}\right)$ columns of its incidence matrix form the incidence matrix of a $\left(2n-1; 2^n + 2^{n-2}, 3\right)$-uniform SS.*

Proof. We know that the lemma is true for $n = 3$, by Example 5. We use the mathematical induction to prove the lemma. Let's assume that there exists a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-$SS$ such that the first $\left(2^k + 2^{k-2}\right)$ columns of its incidence matrix form the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2}, 3\right)$-uniform SS. Let A denote the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-$SS$. Let B denote the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2}, 3\right)$-uniform SS that is formed by the first $\left(2^k + 2^{k-2}\right)$ columns of A. And let c denote the last column of A.

Now construct a $(2k+1) \times \left(2^{k+1} + 2^{k-1} + 1\right)$ matrix D as follows:

$$D = \left(\begin{array}{c|c||c} B & B & c \\ \hline \mathbf{1} & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{1} & 0 \end{array}\right).$$

We know that the first $\left(2^{k+1} + 2^{k-1}\right)$ columns of D form the incidence matrix of a $\left(2k+1; 2^{k+1} + 2^{k-1}, 3\right)$-uniform SS. We will prove that D is the incidence matrix of a $\left(2k+1; 2^{k+1} + 2^{k-1} + 1, 3\right)$-$SS$. Let L_1 denote the first $\left(2^k + 2^{k-2}\right)$ columns of D, let L_2 denote the next $\left(2^k + 2^{k-2}\right)$ columns of D, and let R denote the last columns of D.

1. Three columns from $\{L_1, L_2\}$: (1) is satisfied, since the first $\left(2^{k+1} + 2^{k-1}\right)$ columns of D form the incidence matrix of a $(2k+1; 2^{k+1} + 2^{k-1}, 3)$-uniform SS, (1) is satisfied.

2. Two columns from L_1 and the column R: Since B and c form the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-$SS$, (1) is satisfied.

3. One column from each L_1 and L_2, and the column R: Then (1) is satisfied by taking the last row of D.

4. Two columns from L_2 and the column R: This is similar to the second case.

Therefore, there exists a $\left(2k+1; 2^{k+1} + 2^{k-1} + 1, 3\right)$-$SS$ such that the first $\left(2^{k+1} + 2^{k-1}\right)$ columns of its incidence matrix form the incidence matrix of a $\left(2k+1; 2^{k+1} + 2^{k-1}, 3\right)$-uniform SS. □

The second lemma states that there exists a $\left(2n-1; 2^n + 2^{n-2} + 1, 3\right)$-uniform SS for $n \geq 3$. We prove this by using the (nonuniform) splitting systems constructed in the first lemma.

Lemma 5. *For any integer $n \geq 3$, there exists a $(2n-1; 2^n + 2^{n-2} + 1, 3)$-uniform SS.*

Proof. Actually, we will prove that there exists a $(2n-1; 2^n + 2^{n-2} + 1, 3)$-uniform SS having a column that has only two "1"s.

By Example 3, we know that the lemma is true for $n = 3$. We use the mathematical induction on n. Suppose that the lemma is true for $n = k \geq 4$. By Lemma 4, there exists a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-$SS$ such that the first $\left(2^k + 2^{k-2}\right)$ columns of its incidence matrix form the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2}, 3\right)$-uniform SS. Let B denote the incidence matrix of this $\left(2k-1; 2^k + 2^{k-2}, 3\right)$-uniform SS. And let c denote the last column of the incidence matrix of a $(2k-1; 2^k+2^{k-2}+1, 3)$-SS. Note that c has only two "1"s if we construct a $(2k-1; 2^k + 2^{k-2} + 1, 3)$-$SS$ using the matrix in Example 5.

By the assumption, there exists a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-uniform SS whose incidence matrix has a column with only two "1"s. Let D denote this incidence matrix. By exchanging some rows and columns we can obtain the matrix D' whose first column is the same as c. Let E denote the matrix formed by deleting the first column from D'.

Now construct a $(2k+1) \times \left(2^{k+1} + 2^{k-1} + 1\right)$ matrix A as follows:

$$A = \left(\begin{array}{c||c|c} B & c & E \\ \hline\hline \mathbf{1} & 0 & \mathbf{0} \\ \hline \mathbf{0} & 0 & \mathbf{1} \end{array}\right).$$

We will prove that A is the incidence matrix of a $(2k+1; 2^{k+1}+2^{k-1}+1, 3)$-uniform SS. Let L denote the first $\left(2^k + 2^{k-2}\right)$ columns of A, let R_1 denote the next column of A, and let R_2 denote the next $\left(2^k + 2^{k-2}\right)$ columns of A.

1. Three columns from L: Since B is the incidence matrix of a uniform $\left(2^k + 2^{k-2}, 3\right)$-$SS$, (1) is satisfied by taking one of the first $(2k-1)$ rows of A.

2. Two columns from L and the column R_1: Since $(B|c)$ is the incidence matrix of a $\left(2k-1; 2^k + 2^{k-2} + 1, 3\right)$-$SS$, (1) is satisfied by taking one of the first $(2k-1)$ rows of A.

3. Two columns from L and one column from R_2: Then (1) is satisfied by taking the last row of A.

4. One column from L and two columns from $\{R_1, R_2\}$: Then (1) is satisfied by taking the $2k$-th row of A.

5. Three columns from $\{R_1, R_2\}$: Since $(c|E)$ is the incidence matrix of a $\left(2k-1; 2^k+2^{k-2}+1, 3\right)$-uniform SS, (1) is satisfied by taking one of the first $(2k-1)$ rows of A.

Finally, it is readily apparent that each row of A has exactly $(2^k + 2^{k-2})$ "1"s; therefore, this splitting system is uniform. And the $(2^k + 2^{k-2} + 1)$-th column has exactly two "1"s. Thus, there exists a $(2k+1; 2^{k+1}+2^{k-1}+1, 3)$-uniform SS having a column that has only two "1"s. □

Now we give the odd case of our main theorem. It will be proved by using the previous two lemmas and counting the number of pairs of complementary columns of the constructed splitting systems.

Theorem 10. *For any integer $n \geq 3$, there exists a $(2n-1; 2^n + 2k + 1, 3)$-uniform SS where $0 \leq k \leq 2^{n-3}$.*

Proof. We know that this is true for $n = 3, 4$. Let's assume that $n \geq 5$. There exists a $\big(2n-5; 2^{n-2} + 2^{n-4} + 1, 3\big)$-nonuniform SS such that the first $\big(2^{n-2} + 2^{n-4}\big)$ columns of its incidence matrix form a uniform splitting system and this $\big(2n-5; 2^{n-2} + 2^{n-4}, 3\big)$-uniform SS has 2^{n-4} pairs of complementary columns. It can be made by using Lemma 4 starting from Example 5. Let A denote the matrix formed by the first $\big(2^{n-2} + 2^{n-4}\big)$ columns of the incidence matrix of the above $\big(2n-5; 2^{n-2} + 2^{n-4} + 1, 3\big)$-$SS$. And let c denote the last column.

Furthermore, there exists a $\big(2n-5; 2^{n-2} + 2^{n-4} + 1, 3\big)$-uniform SS such that its incidence matrix has the same column as c. It can be made by using Lemma 5. Let B denote the matrix formed by deleting the same column as c from the incidence matrix of this $(2n-5; 2^{n-2} + 2^{n-4} + 1, 3)$-uniform SS.

We can then construct the incidence matrix of $(2n-1; 2^n + 2^{n-2} + 1, 3)$-uniform SS as follows:

$$\left(\begin{array}{cc||c|cc} A & A & c & A & B \\ \hline \mathbf{1} & \mathbf{0} & 0 & \mathbf{1} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{1} & 0 & \mathbf{0} & \mathbf{1} \\ \hline\hline & \mathbf{1} & 0 & \mathbf{0} & \\ \hline & \mathbf{0} & 0 & \mathbf{1} & \end{array}\right)$$

Since A has 2^{n-4} pairs of complementary columns, this splitting system has at least 2^{n-3} pairs of complementary columns. Therefore we can find a $\big(2n-1; 2^n+2k+1, 3\big)$-uniform SS where $0 \leq k \leq 2^{n-3}$ by deleting $\big(2^{n-3} - k\big)$ pairs of complementary columns from the above splitting system. □

By combining Theorems 9 and 10, and several splitting systems in the appendix, we finally can obtain our main theorem.

Theorem 11. *For any integer $n \geq 4$, there exists a $(2n-1; 2^n + k, 3)$-uniform SS where $0 \leq k \leq 2^{n-1} + 1$.*

5. Conclusion

In this paper, we find new constructions for uniform $(m, 3)$-splitting systems. They improve some of the known upper bounds on the size of such systems. For instance, we improved some bounds of Table 1 in [1] (for $m = 19, 21, 22, 24$). Recently, van Rees and Lau improve the bound for $m = 20$ using disjunct splitting systems [4]. We compare bounds for uniform $(m, 3)$-splitting systems for $m \leq 24$ in Table 1. We also present Table 2 that summarizes our results and compare them with previous results [1].

Asymptotically, van Rees and Lau recently gave a better result that one can construct $\big(4j + 2; 4\big(1.4953^j\big), 3\big)$-uniform SS using disjunct splitting systems [4]. However, there remains a large gap between the lower bounds and the upper bounds for uniform $(m, 3)$-splitting systems. It would be nice if the difference between the two could be bounded by a constant.

m	[1]	Our	[4]
4	2	2	2
5	3	3	3
6	4	4	4
7	3	3	3
8	4	4	4
9	5	5	5
10	5	5	5
11	5	5	5
12	6	6	6
13	6	6	6
14	6	6	6
15	5	5	5
16	6	6	6
17	6	6	6
18	$\geq 6, \leq 7$	$\geq 6, \leq 7$	$\geq 6, \leq 7$
19	$\geq 6, \leq 8$	$\geq 6, \leq 7$	$\geq 6, \leq 7$
20	$\geq 6, \leq 7$	$\geq 6, \leq 7$	6
21	$\geq 6, \leq 8$	$\geq 6, \leq 7$	$\geq 6, \leq 7$
22	$\geq 6, \leq 8$	$\geq 6, \leq 7$	$\geq 6, \leq 7$
23	$\geq 6, \leq 7$	$\geq 6, \leq 7$	$\geq 6, \leq 7$
24	$\geq 6, \leq 8$	$\geq 6, \leq 7$	$\geq 6, \leq 7$

Table 1: *Upper bounds for the number of blocks in $(m, 3)$-uniform SS for $m \leq 24$*

m	[1]	Theorem 8	Theorem 11
2^n	$2n-2$	-	$2n-1$
2^n+1	$2n+2$	$2n-1$	$2n-1$
2^n+2	$2n$	-	$2n-1$
2^n+3	$2n+2$	$2n-1$	$2n-1$
2^n+4	$2n$	-	$2n-1$
2^n+5	$2n+2$	$2n+1$	$2n-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^n+2^{n-1}	$2n$	-	$2n-1$
$2^n+2^{n-1}+1$	$2n+2$	$2n+1$	$2n-1$
$2^n+2^{n-1}+2$	$2n$	-	-
$2^n+2^{n-1}+3$	$2n+2$	$2n+1$	-
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^{n+1}-2$	$2n$	-	-
$2^{n+1}-1$	$2n+2$	$2n+1$	-

Table 2: *Upper bounds for the number of blocks in $(m, 3)$-uniform SS for large enough m*

A. Some examples of splitting systems

Example 6.

$$\begin{pmatrix}
1&1&1&1&1&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0\\
0&1&1&1&0&1&1&0&0&0&0&1&0&1&0&0&1&0&1&0&1\\
1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&1&1&0&0&0&0\\
0&0&0&0&0&1&1&1&1&1&0&1&0&1&1&0&0&0&0&1&1\\
1&0&0&0&1&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0\\
1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

is the incidence matrix of a $(7; 21, 3)$*-uniform SS.*

Example 7.

$$\left(\begin{array}{c|c}
11111100000&11111000000\\
11100011000&11100111000\\
10010011100&11000110110\\
10000000111&00111001111\\
10001111011&00100110001\\
\hline
11111111111&00000000000\\
00000000000&11111111111
\end{array}\right)$$

is the incidence matrix of a $(7; 22, 3)$*-uniform SS. It has* 4 *pairs of complementary columns. And note that the upper left submatrix and the upper right submatrix are the incidence matrices of* $(5; 11, 3)$*-SS (nonuniform).*

Example 8.

$$\left(\begin{array}{c|c}
11111100000111110000000&0\\
11100011000111001110000&1\\
10010011100110001101100&0\\
10000000111001110011111&1\\
10001111011001001100001&0\\
11111111111000000000000&0\\
00000000000111111111111&0
\end{array}\right)$$

is the incidence matrix of a $(7; 23, 3)$*-nonuniform SS. Note that the first 22 columns of this matrix form the incidence matrix of a* $(7; 22, 3)$*-uniform SS.*

Example 9.

$$\begin{pmatrix}
11000110001110001100011\\
10100101001101001010011\\
10010100101100101001011\\
01110000011011100000111\\
00001011101000010111011\\
00000111110000001111101\\
11111000000111110000001
\end{pmatrix}$$

is the incident matrix of $(7; 23, 3)$*-uniform SS.*

Example 10. *The blocks*

$$\{1,\dots,6,12,\dots,16,24,25,29,30,33,34,35,39,40,44,45\},$$
$$\{1,2,3,7,8,12,13,14,17,18,19,23,25,26,27,33,35,36,37,43,44,45\},$$
$$\{1,4,7,8,9,12,13,17,18,20,21,24,27,29,32,33,34,37,39,42,44,45\},$$
$$\{1,9,10,11,14,15,16,19,\dots,23,29,\dots,32,39,\dots,43,45\},$$
$$\{1,5,\dots,8,10,11,14,17,18,22,24,\dots,28,34,\dots,38,45\},$$
$$\{1,\dots,11,28,30,\dots,33,38,40,41,42,44,45\},$$
$$\{12,\dots,22,24,26,29,31,33,34,36,39,41,44,45\},$$
$$\{1,\dots,22\},\ \{24,\dots,45\}$$

form a $(9;45,3)$*-uniform* SS *on the set* $\{1,\dots,45\}$*. It has* 6 *pairs of complementary columns.*

Example 11.

$$\left(\begin{array}{c|c} 111110000000 & 111001101001 \\ 100001110000 & 100110011111 \\ 111001101001 & 111110000000 \\ 011001100110 & 011001100110 \\ 100110011111 & 100001110000 \\ \hline 111111111111 & 000000000000 \\ 000000000000 & 111111111111 \end{array}\right)$$

is the incidence matrix of a $(7;24,3)$*-uniform* SS*. It has* 2 *pairs of complementary columns. And note that the upper left submatrix and the upper right submatrix are the incidence matrices of* $(5;12,3)$*-*SS*.*

Example 12.

$$\left(\begin{array}{c|c} 111110000000 & 111001101001 \\ 100001110000 & 100110011111 \\ 111001101001 & 111110000000 \\ 011001100110 & 011001100110 \\ 100110011111 & 100001110000 \\ \hline 111111111111 & 000000000000 \\ 000000000000 & 111111111111 \end{array}\right)$$

is the incidence matrix of a $(7;24,3)$*-uniform* SS*. It has* 2 *pairs of complementary columns. And note that the upper left submatrix and the upper right submatrix are the incidence matrices of* $(5;12,3)$*-*SS*.*

Example 13. *The blocks*

$$\{1,\dots,5,13,14,15,18,19,21,24\},\ \{1,6,7,8,13,16,17,20,\dots,25\},$$
$$\{1,2,3,6,7,9,12,\dots,17\},\ \{2,3,6,7,10,11,14,15,18,19,21,22\},$$
$$\{1,4,5,8,\dots,13,18,19,20,25\},\ \{1,\dots,12\},\ \{13,\dots,24\}$$

form a $(7;25,3)$*-nonuniform* SS *on the set* $\{1,\dots,25\}$*. Note that it contains a* $(7;24,3)$*-uniform* SS *on the set* $\{1,\dots,24\}$*.*

Example 14. *The blocks*

$$\{5,9,\ldots,12,14,15,16,20,\ldots,23\},\ \{3,4,5,8,11,\ldots,18\},$$
$$\{3,\ldots,7,10,14,15,16,19,24,25\},\ \{1,2,5,\ldots,8,13,14,17,20,21,25\},$$
$$\{1,\ldots,5,9,14,18,19,22,23,24\},\ \{14,\ldots,25\},\ \{1,\ldots,12\}$$

form a $(7;25,3)$*-uniform SS on the set* $\{1,\ldots,25\}$*. It has* 4 *pairs of complementary columns. And note that it contains two* $(5;13,3)$*-SS's on the set* $\{1,\ldots,13\}$ *and* $\{13,\ldots,25\}$ *using the first* 5 *blocks.*

Example 15. *The blocks*

$$\{1,\ldots,5,13,14,15,18,19,21,24,30,34,\ldots,40,44,\ldots,47\},$$
$$\{1,6,7,8,13,16,17,20,\ldots,25,28,29,30,33,36,\ldots,42\},$$
$$\{1,2,3,6,7,9,12,\ldots,17,28,\ldots,32,35,38,39,40,43,48,49\},$$
$$\{2,3,6,7,10,11,14,15,18,19,22,23,26,\ldots,30,34,38,42,43,46,47,48\},$$
$$\{1,4,5,8,\ldots,13,18,19,20,25,26,27,30,\ldots,33,38,41,44,45,49\},$$
$$\{1,\ldots,12,38,\ldots,49\},\ \{13,\ldots,24,26,\ldots,37\},\ \{1,\ldots,24\},\ \{26,\ldots,49\}$$

form a $(9;49,3)$*-uniform SS on the set* $\{1,\ldots,49\}$*. It has* 10 *pairs of complementary columns.*

Acknowledgement

The authors would like to thank the referees for their helpful suggestions.

References

[1] D. Deng, D. R. Stinson, P. C. Li, G. H. J. van Rees, R. Wei, *Constructions and Bounds for* (m,t)*-Splitting Systems*, Discrete Math. **307**(2007), 18–37.

[2] A. C. H. Ling, P. C. Li, G. H. J. van Rees, *Splitting Systems and Separating Systems*, Discrete Math. **279**(2004), 355–368.

[3] D. R. Stinson, *Some Baby-Step Giant-Step Algorithms for the Low Hamming Weight Discrete Logarithm Problem*, Math. Comput. **71**(2002), 379–391.

[4] G. H. J. van Rees, S. J. Lau, $(m,3)$*-Splitting Systems*, Utilitas Math., to appear.